Threat Update Service* Advisory

Protection Pack 2013-11-01-03 Released November 4, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Multiple HP Products CVE-2013-4810 Remote Code Execution Vulnerablilities.

Issue: A remote code execution vulnerability exists in multiple HP products. This could allow a remote attacker to execute arbitrary code on the vulnerable machine via a marshalled object to EJBInvokerServlet or JMXInvokerServlet.

Recommended Action: Apply the specified protection pack (or any later one) and ensure the associated rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	CVE-2013-4810
Advisory	http://h20565.www2.hp.com/portal/site/hpsc/template.PAGE/public/kb/docDisplay/?docId=emr_na-c03897409
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	HP ProCurve Manager (PCM) 3.20 and 4.0 HP PCM+ 3.20 and 4.0 HP Identity Driven Manager (IDM) 4.0 HP Application Lifecycle Management
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-106731
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

